Application. No. 10/081,910

IN THE CLAIMS

1. (Currently Amended) A method for testing randomness when generating a random number, the method comprising the steps of:

generating random sequences of binary bits;

applying said generated random sequences to an exponential overlapping count operation A at a predefined block interval of *k* bits at a time to compute an average number of occurrences for each said predefined block; and

determining whether said generated random sequences are sufficiently random by comparing the output of said exponential overlapping count operation A to a predetermined acceptance range;,

wherein said exponential averaging count operation A is updated according to the following equation:

$$A_{new} = \alpha \bullet A_{old} + b,$$

wherein $\alpha = 1 - 1/n$, and α falls between 0 and 1 ($0 < \alpha < 1$), $n >> 1$, and wherein $b = 1$ if the binary value of the *k* bit block occurs, otherwise $b = 0$.

2. (Original) The method of claim 1, further comprising the step of determining that said generated sequences are sufficiently random when the output of said exponential overlapping count operation A falls between said predetermined acceptance range.

3. (Original) The method of claim 1, further comprising the step of notifying that said generated sequences are not sufficiently random when the output of said exponential overlapping count operation A falls outside said predetermined acceptance range.

4. (Original) The method of claim 3, further comprising the step of generating a new set of random sequences when the output of said exponential count operation A falls outside of said predetermined acceptance range.

5. (Cancelled)

6. (Original) The method of claim 1, wherein said exponential overlapping count operation is performed each time a new random bit is generated by dropping the leftmost bit from said predefined block of *k* bits and appending said new random bit to the right of said predefined block of *k* bits.

7. (Currently Amended) The method of claim [[5]] 1, wherein said predetermined acceptance range is defined as follows:

$[n/2^{k+1} - c\ n/2^{k+1}, n/2^{k+1} + c\ n/2^{k+1}]$,

where *c* is selected to achieve a desired security threshold level.

8. (Currently Amended) A method of testing an output of a random number generator, the method comprising the steps of:

(a) generating a continuous stream of binary bits using said random number generator;

(b) performing and tracking an overlapping exponential count operation on a predetermined block of *k* bits at a predefined time interval for each bit to obtain a corresponding frequency value;

(c) comparing all said computed exponential averaging values A **to** a predetermined acceptance range; and,

(d) determining that said generated binary number are non-random when any one of said computed exponential averaging values falls outside of said predetermined acceptance range**;**

wherein said exponential averaging A is defined by:

$A_{new} = \alpha \bullet A_{old} + b$,

wherein $\alpha = 1 - 1/n$, and α falls between 0 and 1 ($0 < \alpha < 1$), n>>1,

wherein b is a value comprising 1 if the binary value of the *k* bit block occurs in said step (b), otherwise 0.

9. (Original) The method of claim 8, further comprising the step of:

repeating said steps (a) - (c) until any of the said computed exponential averaging value falls outside of said predetermined acceptance range.

10. (Original) The method of claim 9, further comparing the step of notifying that non-random numbers are generated when said computed exponential averaging falls outside of said predetermined acceptance range repeatedly more than a predetermined number of times.

11. (Original) The method of claim 9, further comparing the step of generating a new set of random numbers when said computed exponential averaging falls outside of said

predetermined acceptance range repeatedly more than a threshold value.

12. (Original) The method of claim 8, wherein said random number generator is embedded in a smart card.

13. (Cancelled)

14. (Original) The method of claim 8, wherein said overlapping count operation is performed each time a new random bit is generated by dropping the leftmost bit from said predetermined block of *k* bits and appending said new random bit to the right of said predetermined block of *k* bits.

15. (Currently Amended) The method of claim [[13]] <u>8</u>, wherein said predetermined acceptance range is defined as follows:

$[n/2^{k+1} - c\ n/2^{k+1}, n/2^{k+1} + c\ n/2^{k+1}]$,

where *c* is selected to achieve a desired security threshold level.

16. (Currently Amended) An apparatus for testing the randomness of a random number sequence, comprising:

a random generator unit for generating substantially random sequences of binary bits; and

a detector unit, coupled to the output of said random generator unit, for detecting whether said generated random sequences are sufficiently random;

wherein said generated random sequences are applied to an exponential overlapping count operation A at a predefined block interval of k bits to compute an average number of occurrences for each said predefined block, and wherein if the output of said exponential overlapping count operation A falls outside of a predetermined acceptance range, determining that said generated random sequences are insufficiently random;

wherein said exponential overlapping count operation A is computed according to the following equation:

$A_{new} = \alpha \bullet A_{old} + b$,

wherein $\alpha = 1 - 1/n$, and α falls between 0 and 1 ($0 < \alpha < 1$), n>>1,

b = 1 if the binary value of the k bit block occurs, otherwise b = 0, and

A_{old} is preset initially by an operator.

17. (Original) The apparatus of claim 16, further comprising a switch unit, coupled to the outputs of said random generator unit and said detector unit, for passing said generated random sequences for a subsequent application when said generated random sequences are determined to be sufficiently random.

18. (Original) The apparatus of claim 16, further comprising means for transmitting an alarm signal when the output of said exponential overlapping count operation A falls outside of said predetermined acceptance range.

19. (Cancelled)

20. (Currently Amended) The apparatus of claim [[19]] 16, wherein said predetermined acceptance range is defined as follows:

$[n/2^{k+1} - c\ n/2^{k+1}, n/2^{k+1} + c\ n/2^{k+1}]$,

where *c* is selected to achieve a desired security threshold level.

21. (Currently Amended) A machine-readable medium having stored thereon data representing sequences of instructions, and the sequences of instructions which, when executed by a processor, cause the processor to:

generate a stream of random numbers of binary bits;

compute and track an exponential overlapping count operation on a predetermined block of *k* bits at a predefined time interval for each bit to obtain a corresponding binary value; and

compare all said computed exponential averaging A to a predetermined acceptance range to determine whether said generated random numbers are sufficiently random;

wherein said exponential averaging A is defined by:

$A_{new} = \alpha \bullet A_{old} + b$,

wherein $\alpha = 1 - 1/n$, and α falls between 0 and 1 ($0 < \alpha < 1$), $n >> 1$,

wherein *b* is a value comprising 1 if the binary value of the *k* bit block occurs, otherwise 0.

22. (Original) The machine-readable medium of claim 21, wherein said generated binary

numbers are not sufficiently random when said computed exponential averaging falls outside of said predetermined acceptance range.

23. (Cancelled)

24. (Original) The machine-readable medium of claim 21, wherein said overlapping count operation is performed each time a new random bit is generated by dropping the leftmost bit from said predetermined block of *k* bits and appending said new random bit to the right of said predetermined block of *k* bits.

25. (Currently Amended) The machine-readable medium of claim **[[23]]** **<u>21</u>**, wherein said predetermined acceptance range is defined by:

$[n/2^{k+1} - c \; n/2^{k+1}, n/2^{k+1} + c \; n/2^{k+1}]$,

where *c* is selected to achieve a desired security threshold level.

26. (New) The apparatus of Claim 16, wherein the detector unit comprises a ring buffer and a plurality of accumulators.